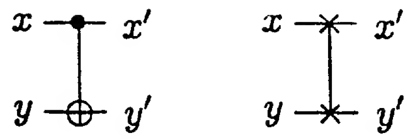

Figure 1

Input: $|\chi\rangle$, $|I_\tau(\chi)\rangle = |0\rangle$, $|w\rangle = |0_{\lceil \log n \rceil}\rangle$

1: for $i = 1$ to n do
2: if $(|\chi_i\rangle = |1\rangle)$ then
3: $|w\rangle \leftarrow |w + 1\rangle$
4: endif
5: endfor

6: if $(|w\rangle \geq |\tau\rangle)$ then
7: $|I_\tau(\chi)\rangle \leftarrow |I_\tau(\chi) \oplus 1\rangle$
8: endif

9: for $i = n$ to 1 do
10: if $(|\chi_i\rangle = |1\rangle)$ then
11: $|w\rangle \leftarrow |w - 1\rangle$
12: endif
13: endfor

Output: $|\chi\rangle$, $|I_\tau(\chi)\rangle$, $|w\rangle = |0_{\lceil \log n \rceil}\rangle$

Figure 2

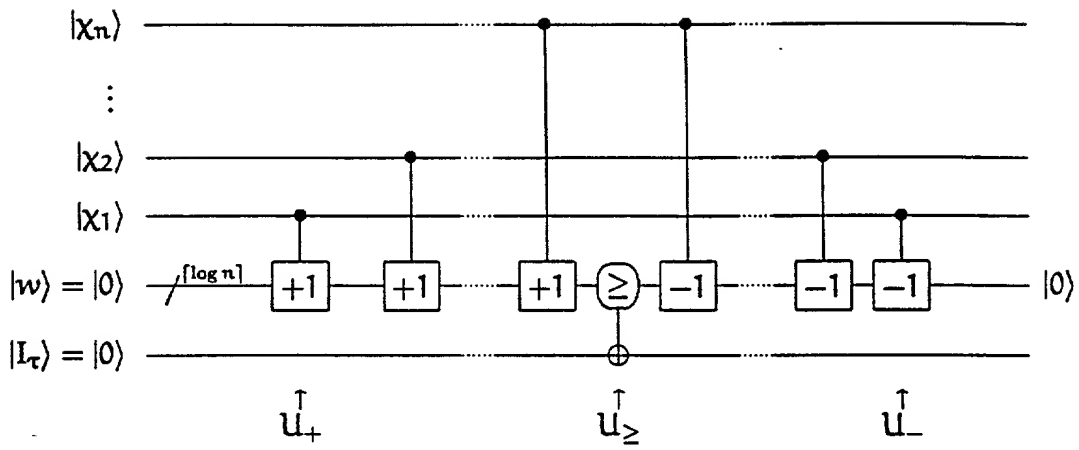

Figure3

Input: $|A\rangle$, $|B\rangle$, $|R\rangle$, i, $|T\rangle = |0_{iq}\rangle$

1: $|R\rangle \leftrightarrow |T_{[(i-1)q+1,iq]}\rangle$
2: for $j = (i-1)q$ to 1 do
3: if $(|A_{[j,j]}\rangle = |1\rangle)$ then
4: $|T\rangle \leftarrow |T + B2^{-j}\rangle$
5: endif
6: if $(|T\rangle \geq |B2^{-j}\rangle)$ then
7: $|A_{[j,j]}\rangle \leftarrow |A_{[j,j]} \oplus 1\rangle$
8: endif
9: $|T_{[iq]}\rangle \leftrightarrow |A_{[iq]}\rangle$
10: endfor

Output: $|A\rangle \leftarrow |AB + 2^{-(i-1)q-1}R\rangle$,
$|R\rangle = |0_q\rangle$, $|T\rangle = |0_{iq}\rangle$

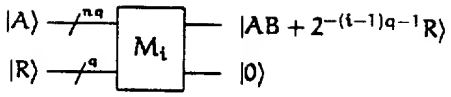

Figure 4

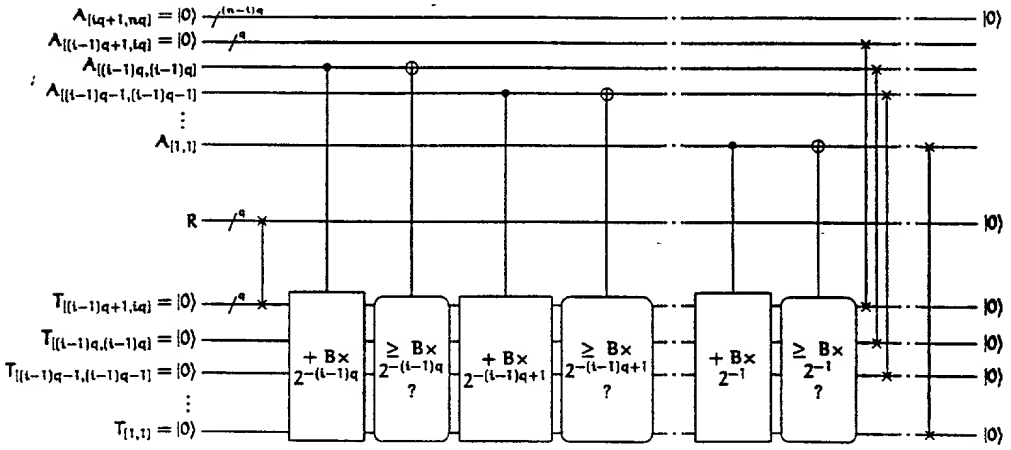

Figure 5

Input: $|\chi\rangle$, $|C\rangle = |0_{nq}\rangle$, $|R_1R_2\cdots R_n\rangle$
$|R\rangle = |0_q\rangle$

E1: for $i = 1$ to n do

E2: $R \leftrightarrow R_i$
E3: if $(|\chi_i\rangle = |0\rangle)$ then
E4: multiply $(|C\rangle, |\lambda_0^\circ\rangle, R, i)$
E5: else
E6: multiply $(|C\rangle, |\lambda_1^\circ\rangle, R, i)$
E7: $|C\rangle \leftarrow |C + \lambda_0^\circ\rangle$
E8: endif

E9: if $(|C\rangle \geq |\lambda_0^\circ\rangle)$ then
E10: $|\chi_i\rangle \rightarrow |\chi_i \oplus 1\rangle$
E11: else
E12: $|\chi_i\rangle \rightarrow |\chi_i \oplus 0\rangle$
E13: endif

E14: endfor

Output: $|\chi\rangle \leftarrow |0_n\rangle$, $|C\rangle$, $|R_1R_2\cdots R_n\rangle = |0_{nq}\rangle$
$|R\rangle = |0_q\rangle$

Input: $|\chi\rangle = |0_n\rangle$, $|C\rangle$, $|R_1R_2\cdots R_n\rangle = |0_{nq}\rangle$
$|R\rangle = |0_q\rangle$

D1: for $i = n$ to 1 do

D2: if $(|C\rangle \geq |\lambda_0^\circ\rangle)$ then
D3: $|\chi_i\rangle \leftarrow |\chi_i \oplus 1\rangle$
D4: else
D5: $|\chi_i\rangle \leftarrow |\chi_i \oplus 0\rangle$
D6: endif

D7: if $(|\chi_i\rangle = |0\rangle)$ then
D8: divide $(|C\rangle, |\lambda_0^\circ\rangle, R, i)$
D9: else
D10: $|C\rangle \leftarrow |C - \lambda_0^\circ\rangle$
D11: divide $(|C\rangle, |\lambda_1^\circ\rangle, R, i)$
D12: endif
D13: $R \leftrightarrow R_i$

D14: endfor

Output: $|\chi\rangle$, $|C\rangle = |0_{nq}\rangle$, $|R_1R_2\cdots R_n\rangle$
$|R\rangle = |0_q\rangle$

Figure 6

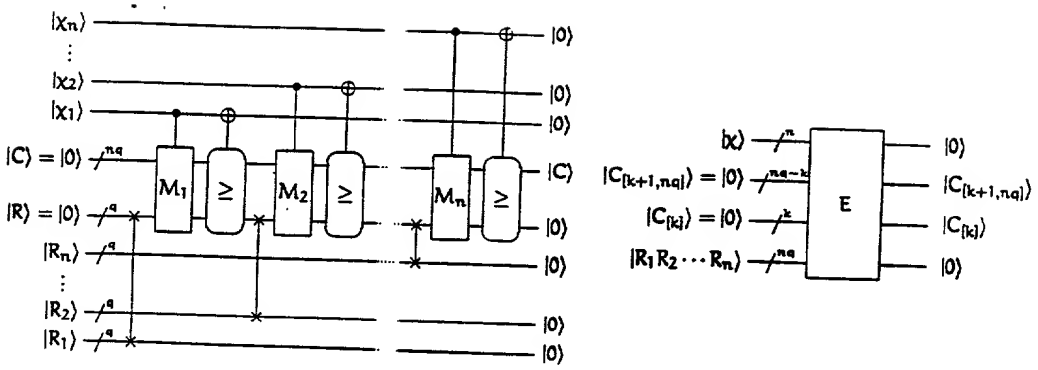

Figure 7

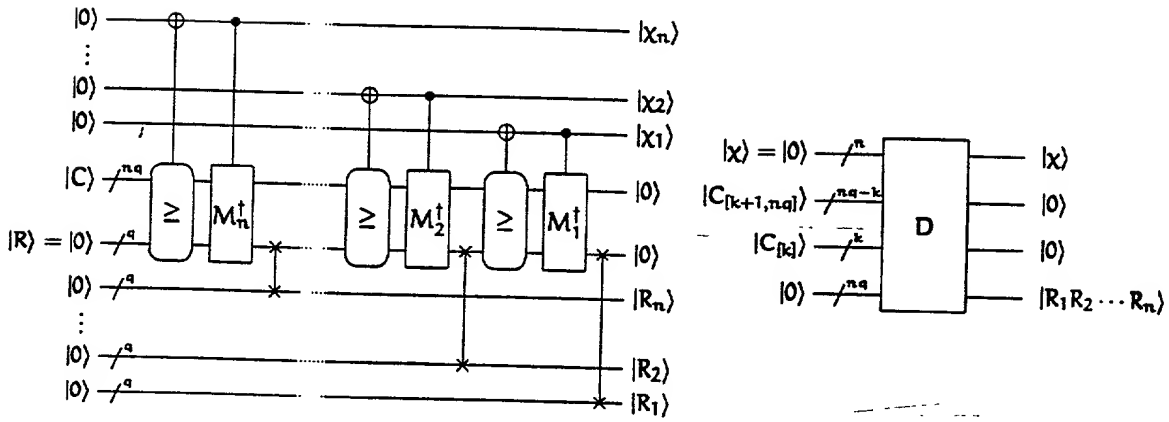

Figure 8

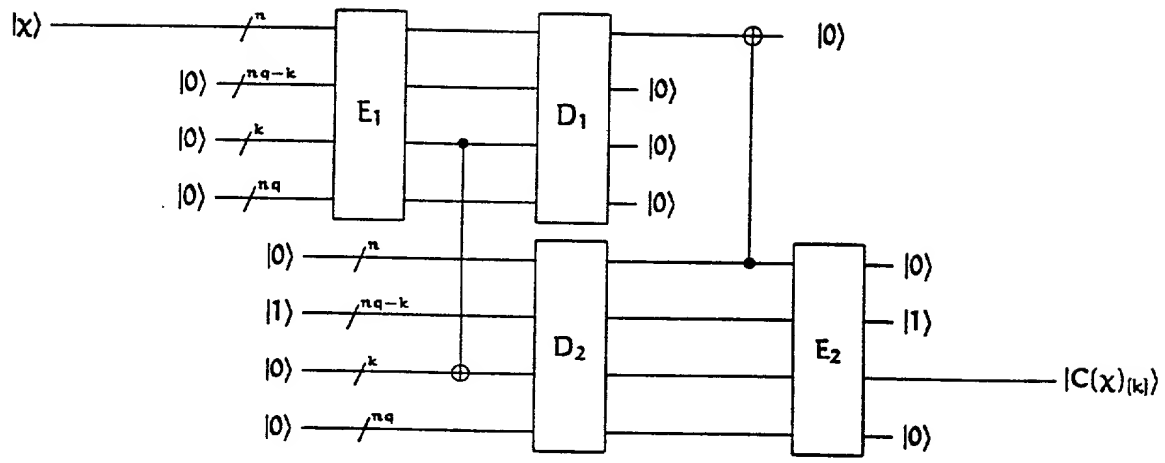

Figure 9